System for Covert Transmission of Data Exploiting ISP Relay Handling of Waveforms of Insufficient Amplitude - Packet Latency Steganography via Fine Control of Power Regulation in Routers

24 August 2024
Simon Edwards
Research Acceleration Initiative

Introduction

Network analysts have struggled in recent years to detect covert transmissions emanating from certain compromised computer systems. While there are many tools available for detecting suspicious network traffic, novel, heretofore undescribed methods are being used to exfiltrate data from secure networks which continue to baffle data engineers by bypassing known methods of detection. A need has been expressed for further information concerning what form this clandestine exfiltration system may take.

Abstract

Certain nation-state entities, i.e. they have a comprehensive understanding of all dimensions of computer and network operations, may be using a novel data smuggling method which evades all known detection methods which exploits knowledge of the behavior of ISP relays in conjunction with knowledge of the voltage control systems of routers.

When an ISP relay receives a signal, it is interpreted and re-transmitted at full amplitude so that it will make the trip to the next relay. What is known to relatively few is that in the protocols used to handle this process, there is a protocol the purpose of which is to alter the protocol of re-transmission in response to low-amplitude signals.

ISPs want to know when there may be trouble with a fiber-optic line and constantly measure the amplitude of incoming signals. The receipt of comparatively few waveforms at a sub-optimal amplitude would trigger a diagnostic process which could be predicted to increase server load and thus increase latency. In the alternate protocol, the number of duplicate bits transmitted is stepped up in order to increase the chances of data being successfully delivered. The result would be that ISP-to-ISP communications would be altered in a way which could be measured through analysis of latency from the other end of a communication. These subtle differences; given that they do not entail any alteration to data content; would not be subject to analysis by military intelligence and would be overlooked.

If a method were used to inflate latency which necessitated the transmission of irregular packets, this would stand out as fairly obvious to analysts and wouldn't be covert. However, an intruder with control over the power regulation system of a router could slightly and briefly decrease the amount of voltage available to

an optical emitter in order to create waveforms which are of sufficient amplitude to be properly interpreted and relayed but which are deficient enough to trigger an automated process at the ISP level meant to diagnose potential problems and to activate alternative transmission protocols.

Conclusion

Thus, an ISP may be spoofed into taking actions which increase latency without the need for data content to be changed, thus allowing for data to be steganographically encoded into latency variations and covertly exfiltrated from secure systems.